Testimony of Dr. José-Marie Griffiths

before the United States Senate Committee on Agriculture, Nutrition, and Forestry on

"Innovation in American Agriculture: Leveraging Technology and Artificial Intelligence"

Tuesday, November 14, 2023

Dr. José-Marie Griffiths
President
Dakota State University
820 N. Washington Ave.
Madison, SD 57042

Introduction

Chairwoman Stabenow, Ranking Member Boozman, and Members of the Committee, thank you for the opportunity to testify about leveraging technology and artificial intelligence (AI) to drive innovation in American agriculture.

I am Dr. José-Marie Griffiths, President of Dakota State University (DSU) in Madison, South Dakota. At DSU, we are training the next generation of professionals in emerging technology fields such as AI, cyber, and quantum computing. My career has focused on research, teaching, public service, corporate leadership, economic development, and higher education. I have served appointments to the National Security Commission on Artificial Intelligence (NSCAI), National Science Board, President's Information Technology Advisory Committee, and several other federal commissions and committees.

South Dakota is one of the nation's top agricultural states. As a leading research institution for technology education, DSU views agriculture through the lens of innovative applications in cyber, AI, and how to move the industry to the next phase of growth. In collaboration with South Dakota State University (SDSU), the state's leading agricultural institution, we are working to engage in collaborative research through a precision agriculture cyber (CyberAg) partnership; SDSU brings the data generated by precision technologies and DSU brings the cyber and AI expertise.[1] The CyberAg partnership is made possible by a $1.25 million investment from the South Dakota Legislature to begin to develop undergraduate and graduate curricula, engage in research, and provide outreach programming and communication to address agriculture security threats.

At DSU, our mission is to grow future technology talent and help them find rewarding employment inside South Dakota and in other key cyber markets, even beyond the mainstay tech hubs of Silicon Valley and Washington, D.C. We are only one of ten universities nationwide to hold all three Centers of Academic Excellence in Cybersecurity designations from the National Security Agency (NSA). Our innovative R&D campus facilities and public-private partnership models empower students to immediately enter the cyber workforce upon graduation. One such example is the Dakota State University Applied Research Corporation (DARC) which operates and manages the Dakota State University Applied Lab (DSU-ARL).

We currently have a 99.7 percent overall job placement rate that is supporting a skilled talent pipeline of recent undergraduate and graduate students who are ready to address some of the toughest challenges and exciting opportunities posed by AI and emerging technologies.

The Challenge

As a sector, agriculture has evolved tremendously over the past 100 years. Technology is now being leveraged to drive farming equipment, predict crop health and optimize yields, and monitor the entire produce supply chain from seed to stomach.

We must ask ourselves, what does an increase in connectivity and a heavier reliance on technology mean for the future of agriculture? There are tremendous opportunities, and with that,

[1] Amazing Madison. Governor signs bill supporting CyberAg partnership initiative.

there are also risks. With each connected tool or vehicle, the potential attack surface grows, providing multiple entry points for bad actors.

By discussing how to best leverage technology and AI for innovation in agriculture, we can consider the benefits to modern practices, the impact on the cyber threat landscape, and what further research is needed to reach full innovative potential.

Benefits and Considerations for Precision Farming

Modern farming, often referred to as "precision agriculture" or "precision farming," has come a long way from the traditional practices of the past. This transformation has been made possible with the integration of cutting-edge technologies including AI, robotics, cloud computing, smart sensors, and actuators.

The U.S. Department of Agriculture (USDA) has reported a substantial increase in the adoption of precision technologies in agriculture since the mid-1990s. For example, auto-steer and guidance systems are now used on over 50% of U.S. acres planted with crops like corn, soybeans, winter wheat, cotton, rice, and sorghum. This is up from roughly 10% of planted acres or fewer in the early 2000s.[2]

The increased adoption of AI signifies its transformative potential in the U.S. agriculture sector. When embedded in connected systems, AI technologies enable the widespread collection of vast amounts of data from crops and livestock through satellites, drones, sensors, and robots, which in turn help lower costs and improve yields and production.[3]

Potential Impacts

The Senate Committee on Agriculture, Nutrition, and Forestry published statistics that show farm production expenses are projected to be record-high in 2023 at nearly $500 billion, up by 28% or $87 billion.[4] Today, agricultural producers are constantly seeking innovative ways to lower such costs and improve productivity and yields. AI presents incredibly promising solutions for these needs.

For example, autonomous tractors, combines, or other farming equipment with integrated AI technology, such as the auto-steer and guidance systems previously described, can help reduce the cost of labor and other operating costs, as this machinery can work tirelessly without the constraint of human fatigue. The combination of AI and precision agriculture could reduce the operating costs of corn, soybean, and wheat production in the United States by 26%, 31%, and 31%, respectively, on a per-acre basis.[5]

---

[2] McFadden, J., Njuki, E., and Griffin, T. February 2023. Precision Agriculture in the Digital Era: Recent Adoption on U.S. Farms. USDA Economic Research Service.
[3] Halverson, T., Rimal, B., and Wang, Y. June 30, 2023. Cybersecurity in precision agriculture: Safeguarding America's connected fields. Infosecurity Magazine.
[4] U.S. Senate Committee on Agriculture, Nutrition, and Forestry. May 9, 2023. Revisiting Farm Production Expenses.
[5] Maguire, D. August 2, 2023. Will the Convergence Between Artificial Intelligence and Precision Agriculture Lower Farming Costs? ARK Invest.

Additionally, successful crop cycles are critically dependent on technology. AI's predictive capabilities allow valuable insights on crop health, market demand, and weather patterns using both historical and real-time information. This empowers agricultural producers to make informed decisions in optimizing fertilizer, watering, and other practices for better crop yields and profitability.

Recommendations

While there is a vast potential for AI and digital technology in farming today and in the future, many of these digital tools have significant up-front costs, repair or replacement expenses, and annual user fees. These costs can present a barrier to adoption for farmers, making USDA's conservation programs that provide technical or financial assistance to farmers seeking to implement digital agriculture technologies increasingly critical. Continued support for these programs is essential to ensure the sustainable growth of AI in agriculture as we usher in a new era of innovative farming solutions.

Cyber Security and Intelligence Risks to Address

There is a real need for stronger cyber security protections to safeguard U.S. agriculture and critical infrastructure that power our national food supply. Looking through the lens of cyber security, the deeper we embed AI into internet-connected farming machinery, vehicles, and devices, the more vulnerable these systems become to cyberattacks.

On September 1, 2021, the FBI released a notification report sounding the alarm on cybercriminals increasingly targeting the food and agriculture sector due to the rise in adoption of smart technologies and the internet of things (IoT).[6] For reference, six attacks against grain cooperatives occurred in the fall of 2021.[7] In early 2022, two agriculture related attacks occurred that temporarily disrupted seed and fertilizer supply.[8] Later that year, the FBI reported a total of 48 ransomware attacks targeting the food and agriculture industry during 2022.[9] The increasing frequency of attacks on this sector further underscores the national and economic security risks that need to be addressed.

Intellectual property (IP) confidentiality risk is another consideration which has come up in my conversations with both public and private stakeholders regarding agriculture technologies. As AI applications are rapidly developed and deployed, IP confidentiality is essential to protect and prioritize further development of leading innovations in the field.

Furthermore, a heightened concern for cyber and national security involves the acquisition of land by unfriendly nations, especially in sensitive areas or close proximity to critical infrastructure and agricultural areas. Of particular significance is the safeguarding of seed vaults or banks, which are often overlooked as critical infrastructure but are essential as a vital resource. These vaults play a crucial role in the agriculture industry, serving as the starting point for both the supply and food chains within the sector.

---

[6] FBI. September 1, 2021. Private Industry Notification.
[7] Reed, J. September 14, 2022. Ransomware attacks on agriculture potentially timed to critical seasons. Security Intelligence.
[8] Michigan Farm News. April 22, 2022 FBI Alert: Ag ransomware attacks timed to critical seasons.
[9] FBI. 2022 Internet Crime Report.

Presently, China possesses 380,000 acres of U.S. land.[10] In 2021, a Chinese company acquired land near a Grand Forks, North Dakota Air Force base, sparking concern among lawmakers.[11] This raises apprehensions about China having the capacity and capability to control the U.S. food and energy supply, as well as highly sensitive sites that can influence markets and impact critical infrastructure. As geopolitical tensions escalate, it becomes crucial to secure our land for the sake of our national security.

Potential Impacts

The consequences of heightened cyber security risks accompanying the deployment of AI in agriculture are too significant to overlook. Failure to adequately secure our systems invites hacking attempts on interconnected farming machinery and platforms. This could result in the manipulation of computing in farm equipment, control over water sources, fertilization, treatment of seed stock, and other vital systems. Potential outcomes could include substantial disruptions and harm to livestock, crop health, and the risk of disrupting entire ecosystems and supply chains.

Additionally, the foreign ownership of land near U.S. critical infrastructure, sensitive sites, and farmlands introduces the risk of foreign surveillance, attacks on critical infrastructure such as power, water, and chemical plants, and/or the potential theft of IP—an expensive and challenging setback from which to recover. The consequences are severe, with the Commission on the Theft of American Intellectual Property reporting annual losses of up to $600 billion.[12] This staggering figure is unsurprising, given the numerous cyberattack surfaces inherent in distributed research.

Recommendations

Limited awareness among agricultural producers and stakeholders regarding cyber threats increases their vulnerability and reduces the likelihood of implementing appropriate security measures. It is essential for farmers and agricultural stakeholders to engage actively with and reference the Food and Agriculture Sharing and Analysis Center.[13] This proactive involvement will significantly decrease the risks posed to their operations and contribute to enhancing overall industry security.

The Cybersecurity & Infrastructure Security Agency (CISA), collaborating with the Food and Drug Administration (FDA), the United States Department of Agriculture (USDA), and the Department of Homeland Security (DHS), provides a valuable resource known as the Food and Agriculture Sector-Specific Plan.[14] However, given the substantial changes and technological advancements in the industry since its 2015 publication, an update to this plan is imperative. This

[10] Bustillo, X. and Hanzhang Jin, C. June 26, 2023. China owns 380,000 acres of land in the U.S. Here's where. NPR.
[11] China owns 380,000 acres of land in the U.S. Here's where. NPR.
[12] Badders, T. February 22, 2023. Intellectual property theft: A threat to the U.S. economy and national security. Telos.
[13] Starks, T. May 24, 2023. The food and agriculture industry gets a new center to share cybersecurity information. The Washington Post.
[14] FSA, USDA, and DHS. 2015 Food and Agriculture Sector-Specific Plan.

would serve as a pivotal and relevant resource for the evolving landscape of the agriculture industry.

Increased research in this field holds the potential to proactively prevent cyberattacks. Collaborative efforts between industry and academia can drive innovation and devise preemptive solutions. Notably, the partnership between South Dakota State University (SDSU) and Dakota State University (DSU) is actively exploring vulnerabilities in the agricultural sector, simulating potential attacks, and scrutinizing the security of autonomous vehicle sensors and systems. Supporting additional research within specific cyber practices is crucial to effectively mitigate risks in the evolving landscape of agricultural cyber.

While layered defenses and zero-trust strategies, including solutions like multi-factor authentication (MFA), are vital to safeguard infrastructure in high-risk environments like food production centers and even research institutions, the escalating threats to IP indicate further innovation is necessary to counter determined adversaries who work to find ways to bypass or hack these defenses.

Importance of Sustained Research

Agricultural research, particularly in the realm of AI, is crucial for the sustainability and development of the agriculture industry. This research leads to the creation of new technologies and improved policies that enhance agricultural productivity and resilience.

Collaboration between industry and academia is vital to effectively disseminate AI knowledge and technology. Leading universities like SDSU and DSU are actively engaged in AI research for agriculture, exploring advancements and vulnerabilities associated with AI adoption. Specific projects are focused on investigating sensor technology, vehicles, and GPS systems. Other universities, such as Purdue, have received grants to establish AI Institutes dedicated to climate-smart agriculture and forestry, a prime example for academia's capabilities.[15]

Potential Impacts

Specific research projects between SDSU and DSU include efforts to ensure agricultural data confidentiality and integrity to improve data privacy and secure GPS data integrity from satellite to the cloud. Other projects are designed to develop secure cyber infrastructure for precision agriculture. The proposed integration involves four critically important areas: cyber issues, precision farming data analysis, a portal for agricultural producers, GIS data analysis, and optimization. Full integration of these components will result in new and secure cyberinfrastructure based on resilient networks, optimized energy consumption, and reliable communications. This research has the potential to reduce risks and contribute to the future of the agriculture industry.

The National Institute of Food and Agriculture (NIFA) supports AI and agriculture research, particularly in areas such as agricultural systems, engineering for crop and soil monitoring using technologies like machine learning, remote sensing, satellites, drones, and precision methods.[16]

[15] Purdue University. Purdue receives $500,000 grant as part of new AI Institute focusing on climate-smart agriculture and forestry.
[16] USDA National Institute of Food and Agriculture. General information on artificial intelligence activities.

Additional investment in research is essential for the advancement of smart agricultural systems. Furthermore, research focused on AI applications to aid decision-making by farm, forest, and ranch managers is crucial to sustain and advance the future of the agriculture industry.

Recommendations

According to the Artificial Intelligence R&D Interagency Working (IWG) group, key areas of focus for federal coordination and collaboration on AI include making long-term investments in fundamental and responsible AI research, ensuring the safety and security of AI systems, developing shared public datasets and environments for AI training, and testing, measuring, and evaluating AI systems through standards and benchmarks to expand public-private partnerships to accelerate AI advancements.[17] Effectively addressing these key areas of focus is crucial for advancing agricultural research and the collaboration needed to further fuel the industry.

In line with the USDA's Urban Service Centers and the U.S. Economic Development Administration's (EDA) recent Tech Hubs Program aimed at boosting the technological ecosystem for the U.S. to achieve global leadership, similar hubs or regions should be established for research in AI and agriculture. These designated areas could play a crucial role in advancing our understanding and implementation of AI in agriculture. Moreover, they have the potential to generate a significant number of jobs, ranging from hundreds to thousands, fostering both technological innovation and economic growth, particularly for rural areas like South Dakota.

Supporting research on AI's role in agriculture is critical to ensuring the industry's security and growth. It is also crucial for our nation's innovation and national security, addressing industry challenges and fostering economic growth.

Conclusion

The U.S. has a critical opportunity to advance the deployment of AI to further innovate the agriculture sector while also helping address the very real cyber risks and challenges associated with a growing attack surface. There are crucial steps that academia, in partnership with industry and federal agencies, can take to ensure the safe, responsible, and effective use of AI. The important thing to remember is that the industry has been automating and innovating within the agriculture industry for decades. While the deployment of AI across agriculture is a transformative shift, it is nothing we can't be prepared for.

While this is a complex undertaking that will involve many different players at all levels of both the public and private sectors, we must move forward by addressing the cyber risks and advancing the crucial role of academia in devising research-driven solutions to the agricultural system. Academia has a critical role to play in advancing the next generation of AI literate talent equipped to help the agriculture industry move into the next phase of growth and development.

Chairwoman Stabenow, Ranking Member Boozman, and Members of the Committee, thank you again for this opportunity. I also want to thank our leaders in South Dakota, including Senator Thune, Senator Rounds, Representative Johnson, and Governor Noem for their continued

[17] NITRD. Artificial Intelligence R&D Interagency Working Group.

innovative leadership to drive South Dakota into a new era of innovation. DSU looks forward to continued collaboration with the Committee to help further devise solutions to agriculture's most pressing challenges and ensure that the power of AI can be harnessed to its full potential.

###

Dr. José-Marie Griffiths is the President of Dakota State University in Madison, South Dakota. Dr. Griffiths has spent her career in research, teaching, public service, corporate leadership, workforce and economic development, and higher education administration with a special focus on work in STEM fields. She has served in presidential appointments to the National Science Board, the President's Information Technology Advisory Committee, and the U.S. National Commission on Libraries and Information Science. She was also a member of the National Security Commission on Artificial Intelligence.